PRAGMA
SECURING YOUR DIGITAL FUTURE

HOLLAND & MARIE

PRACTICAL COMPLIANCE AND THE PAYMENT SERVICES ACT:

Complying with the Technology Risk Management Notice And Guidelines

24 February 2020

*The relevant forms and guidelines for the Payment Services Act (the "**PS Act**"), including the main license application form ("**Form 1**")[1] have been published by the Monetary Authority of Singapore (the "**MAS**"). Over the coming weeks, we intend to publish a series of articles considering various practical issues relating to applying for a license under or complying with the PS Act.*

[1] See https://www.mas.gov.sg/-/media/MAS/Sectors/Forms-and-Templates/Form-1---Application-for-a-Payment-Service-Provider-Licence.pdf

INTRODUCTION

We are not going to lie. This article makes technology risk management ("**TRM**") seem impossible.

It is not impossible… but it is not easy either.

TRM involves a mix of technology, financial, operational and compliance considerations. TRM is arguably the most complex risk issue a payment service provider (a "**PSP**") has to assess in its business. The biggest challenge is to develop a sound and robust TRM framework such that a PSP can be confident that it has managed its technology risks in a "systematic and consistent manner" [2] keeping in mind that (1) the potential severity and type of technology threats that PSPs face are constantly changing and (2) the PSP's TRM framework is expected to be commensurate with the level of risk and complexity of the services it offers and the technologies supporting such services.[3]

REGULATORY BACKDROP

For a PSP preparing to apply for a license under the PS Act, we recommend reviewing the following materials [4] as you prepare your TRM framework (which is generally required to be in place at the time of submission of Form 1)[5]

- The TRM Notice 2013
- The TRM Guidelines (the "Guidelines")[6] and ancillary documentation published in 2013. Checklist for the Guidelines (the "Checklist");
    1) Please note that this checklist should be completed each year by senior officers who have director knowledge of the PSP's information systems and operations, and also reviewed by their superiors.[7]
    2) The checklist includes well over 100 TRM issues to consider, plus six appendices.
    3) Instructions on Incident Notification and Reporting to MAS.
    4) FAQ's - Notice on TRM.
- The MAS's latest consultation paper on proposed revisions to the Guidelines (the "2019 TRM Consultation Paper") published in March 2019;
- Notice PSN05 on Technology Risk Management published in 2019 ("PSN05"); and
- The MAS' FAQ on the Payment Services Act (the "PS Act FAQ") which includes a discussion of technology and cyber risk.

As an executive summary of the above, PSN05 sets out requirements of for a high level of reliability, availability and recoverability of critical IT systems and for PSPs to implement information technology controls to protect customer information from unauthorised access or disclosure). The Guidelines set out risk management principles and best practice standards that PSPs should adopt commensurate to the complexity of their operations.

Reviewing these materials will provide a PSP with a strong foundation to consider related notices and guidelines such as:

- MAS' business continuity guidelines;
- a consultation paper on proposed revisions to these guidelines was published in 2019;
- the MAS' Proposed Guidelines on Individual Accountability and Conduct;

[1] See https://www.mas.gov.sg/-/media/MAS/Sectors/Forms-and-Templates/Form-1---Application-for-a-Payment-Service-Provider-Licence.pdf
[2] See Paragraph 4.0.1 of the MAS TRM Guidelines 2 (as defined herein).
[3] See Question 7.26 of Form 1.
[4] All these materials are available on the MAS' website – www.mas.gov.sg
[5] See Question 7.26 of Form 1.
[6] See https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-6 Guidelines--21-June-2013.pdf?la=en&hash=813413DFB093943558376148934CF9AA44F26FB5
[7] See Instruction #1 to the Checklist, which can be found at https://www.mas.gov.sg/regulation/forms-and-templates/checklist-for-technology-risk-management-guidelines

- the MAS' Outsourcing Guidelines (relevant if a PSP plans to outsource any technology functions);
- the MAS' e-Payments User Protection Guidelines;
- Notice PSN06 on Cyber Hygiene which goes into effect on 6 August 2020; and other circulars the MAS has issued on matters such as vulnerability assessments and penetration testing, early detection of cyber intrusion.

THE MAS' FOCUS WITH RESPECT TO TECHNOLOGY

Technology risk was one of the four key risks the MAS identified with respect to regulating PSPs. In particular, the MAS has highlighted the following areas of focus;[8]

- Governance;
- User authentication;
- Cyber hygiene;
- Encryption; and
- Anti-fraud

EMERGING TECHNOLOGY RISKS

Wearables: Apple Watch, Fitbit, Google Glass, and other wearables can expose companies to invasion of privacy and unforeseen dangers.

Internet of Things ("IoT"): The risks stemming from the use of IoT are very new and have grown exponentially over the last three years due to the sheer number of technologies available, from cameras, locks, to home automations systems. The ability to remotely control electronic devices raises privacy and other concerns. Meanwhile, physical risks exists relating to devices which monitor temperature and could overheat or explode.

Cloud Computing: Many organisations incorrectly believe that Cloud is natively secure. This is not true. The risks that exist with on-premise services exist in cloud computing too, and PSPs are required to implement appropriate controls to mitigate them. Types of risk include:

- unauthorised access to customer and business data;
- lack of availability of technology resources and data;
- incomplete data deletion;
- tertiary vendor risks;
- unauthorised access to credentials;
- comingling of data; and
- physical security risks.

In addition, the MAS also addresses cloud computing in its Guidelines on Outsourcing. So PSPs that intend to utilise cloud computing should also consider outsourcing risks.

[8] See https://www.mas.gov.sg/-/media/MAS/FAQ/Payment-Services-Act-Infographic.pdf?la=en&hash=D4635EDDB0CFB4AE8B1022D0E76F428E09B4F9BF

Quantum Computing: The next evolution of technology "more processing speed" will probably happen as a result of drops in pricing for Quantum computers. Quantum computers will stimulate the development of new breakthroughs in science, machine learning methods to diagnose illnesses faster, new machine made materials, financial strategies, and algorithms. However, the sudden access to Quantum computers will render all the encryption algorithms used to date vulnerable, making current implementation of HTTPS, and SSL open to abuse. Governments , beware all previously encrypted information will be open to brute force attacks that will take minutes not trillion years to decrypt.

Artificial intelligence ("AI"): The simulation of human intelligence in machines that are programmed to think like humans and mimic their actions is already taking place (see ridesharing apps like Uber). The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving. The risk is what happens if we cannot control how the AI thinks and what it does or create....Yes, we believe that the true villain of the Terminator films is the COO who failed to implement a proper TRM framework for Skynet!

An example of a more immediate concern is Google Translate. Google Translate is AI driven system that supports multiple language translations. Google has announced that the Google AI has created its own language to support new translations. However, no human can understand or use this new language. Presumably, Google didn't plan for that to happen.

KEY CONSIDERATIONS WHEN PREPARING YOUR TRM POLICIES AND FRAMEWORKS

1. Have a framework to discern what technology/system is critical to your business - Is the technology relevant to your business from a financial perspective? Would a failure impact your operations or affect your customers' data?
2. Ensure your critical technology is available for more than 99.954% of the time in each 12 month period (not more than four hours on a rolling 12 month basis).
3. Have a requirement to notify the MAS within 60 minutes of discovering a cyber security breach or an incident that has impacted your critical technology/systems. A report identifying the root cause analysis should be shared with the MAS within 14 days.
4. Implement information technology controls to protect customer information from unauthorised disclosure. There are approximately 400 controls identified in the Checklist that "senior officers who have direct knowledge" of a PSP's information systems and operations should consider each year. The Checklist includes questions about:
    - Threat and vulnerability risk assessments;
    - Monitoring privileged accounts;
    - Implementation of perimeter security for your critical assets; and
    - Reviewing access controls and document security standards.
5. Implement a "RACI Matrix" (see example next page). The 2019 TRM Consultation Paper states that a PSP may wish to consider delineating the roles and responsibilities for technology risks using a RACI matrix[9]. A RACI matrix is a chart that maps out every task, milestone or key decision involved in completing a project. The RACI matrix assigns which roles are responsible for each action item, which personnel are accountable, and who needs to be consulted or informed. Establishment of a RACI matrix relating to technology risks should help demonstrate that the Board of Directors and Chief Executive Officer of a PSP demand accountability in terms of identifying and addressing technology risks.

[9] RACI is an acronym for "Responsible", "Accountable", "Consulted" or "Informed".

	ROLES	Sponsor	Leader A	Player 1	Player 2	Player 3	Player 4	Player 5	Player 6	Auditor 1	Auditor 2
	Deliverable or Task	Status	Sponsor/Leadership		Project Team					Audit Team	
	Scope 1 - Security Design										
	Designing the Architecture			I	A	R	R	S	S	S		
	Documenting the Design			I	A	R	R	D	S	S		
	Working Solutions			I	A	R	R	I	S	S		
	Scope 2 - Documentation										
	Document Policies and Procedures			I	A	C	D	R	S	S		
	Scope 3 - Security Assessment										
	Testing Internally and Externally			I	A	C		R	S	I		
	Report Pre and Post Fixes			I	A	R		C	S	S		
	Scope 4 - IT Security Audit										
	IT Security Audit			I	A	C	C	C	C	I	A	R
	Fix Issues			I	A	R	R	R	R	R		
	IT Security Audit Report			I	A	I	I	I			A	R

D	Driver	Assists those who are responsible for a task.
R	Responsible	Assigned to complete the task or deliverable.
A	Accountable	Has final decision-making authority and accountability for completion. Only 1 per task.
S	Support	Provides support during implementation.
C	Consulted	An adviser, stakeholder, or subject matter expert who is consulted before a decision or action.
I	Informed	Must be informed after a decision or action.

THE HIGH STAKES OF TRM

Irrespective of the regulatory requirements, TRM is important because it mitigates risks that will adversely affect your revenues and customers.

However, if you only want to consider the adverse regulatory outcomes, potential disciplinary consequences include:

- Suspension of license until a problem is adequately addressed;
- Revocation of licence
- Public warning including details about the technology incident and governance failures; and
- Financial penalties.

[9] RACI is an acronym for "Responsible", "Accountable", "Consulted" or "Informed".

Irrespective of the regulatory requirements, TRM is important because it mitigates risks that will adversely affect your revenues and customers.

However, if you only want to consider the adverse regulatory outcomes, potential disciplinary consequences include:

- Suspension of license until a problem is adequately addressed;
- Revocation of licence
- public warning including details about the technology incident and governance failures; and
- Financial penalties.

CONCLUSION

TRM is a subject that requires a range of stakeholders to work together. You need advisors who:

- are experts at identifying and solving technology and cyber-security issues and aware of the latest threats and solutions; and
- have compliance and ideally senior management (chief operating officer/chief executive officer) expertise who can properly advise a PSP's board of directors on its responsibilities and governance relating to TRM.

Fortunately, the combination of Pragma and Holland & Marie offers all that capability, and more! If you are interested to explore how we may be able to assist you with your TRM framework, please reach either firm at our details below.

For further information, contact:

Chris Holland: Partner | Holland & Marie | 201802481R
7 Straits View, Marina One East Tower, #05-01 Singapore 018936
www.hmcompliance.com

Manish Chawda: Partner | Pragma | 201629205M
35A Keong Saik Road, #03-00. Singapore 089142
www.pragmastrategy.com

PRAGMA SECURING YOUR DIGITAL FUTURE

HOLLAND & MARIE